

Exhibit 29

Excerpts of SW-SEC00648038

Attorney Client Privileged / Attorney Work Product

		Evaluation of ITGC Deficiencies	
Prepared by	Reviewed by	Date	Period-end
Internal Audit / KPMG	Bart Kalsu, EVP, CFO	02/23/2020	12/31/2020

Purpose

This memo is intended to summarize management's evaluation of the severity of the IT general control deficiencies identified in SolarWinds Inc.'s (the Company) internal control over financial reporting (ICFR) as of December 31, 2020 (FY 2020) for consideration in the determination of the effectiveness of ICFR disclosed by management in Item 9A of Form 10-K, with particular focus on the ICFR implications of the cybersecurity event identified during FY 2020

Management is required to evaluate the severity of a deficiency in ICFR by considering whether there is a reasonable possibility that the entity's ICFR will fail to prevent or detect a material misstatement of the financial statement amount or disclosure; and the magnitude of the potential misstatement resulting from the deficiency¹. The 2013 COSO Framework also requires management to assess the severity of identified control deficiencies². Management utilized a six step process to identify and evaluate internal control deficiency/(ies). Considerations related to each step in that process are documented below.

Step 1 -- Describe the control deficiency

The Company's environment was compromised through a sustained series of malicious activities which resulted in inappropriate access to certain privileged and generic accounts. These activities resulted in unintended authentication by outside threat actors to SolarWinds' IT systems. As a result, the following design deficiencies were identified, :

- Lack of adequate preventative and/or detective authentication controls over domain administrator accounts to restrict access to financial reporting infrastructures to only approved and authorized users
- Lack of adequate preventative and/or detective authentication controls over user accounts to restrict access to financial reporting systems to only approved and authorized users

Through management's event investigation / analysis efforts, management noted that certain accounts were associated with Indicators of Compromise (IOC), such that all activity performed by these accounts was not assured of being performed as intended by the authorized account user. These accounts included certain Window administrative accounts (5), a generic service account (1), a generic email account (1), and certain user accounts (4). An additional impact was noted where the 1 compromised email account was able to view the email activity of 71 additional users. However, none of these user accounts were specifically accessed through compromised credentials.

Based on the identification of these compromised user id's, management concluded that the attributes lacked specificity in the designed control to effectively protect financial systems from perimeter cyber

¹ 17 CFR Part 241, Commission Guidance Regarding Management's Report on Internal Control over Financial Reporting Under Section 13(a) or 15(d) of the Securities and Exchange Act of 1934, p. 35

² COSO Internal Control-Integrated Framework (2013). See principle 17

Attorney Client Privileged / Attorney Work Product

- modified configurations, report structures, or underlying data as it relates to the completeness and accuracy of IPE
- unauthorized transaction approvals
- access to modify wire-related access (including the ability to setup or modify vendors) was changed

The specific business controls considered in this analysis are available below (See *Appendix B*). Specific consideration of how these controls impact specific risks is available in the detailed testing found in the various analysis packages.

Material Weakness Considerations

Our evaluation of the severity of the deficiency considered the indicators of a material weakness in AS 2201.69:

- Identification of fraud, whether or not material, on the part of senior management;
 - *Through the course of management's investigation of the cybersecurity event, there is no indication of fraud on the part of management associated with this event.*
- Restatement of previously issued financial statements to reflect the correction of a material misstatement;
 - *There has been no identified financial statement misstatement as a result of the cybersecurity event.*
- Identification by the auditor of a material misstatement of financial statements in the current period in circumstances that indicate that the misstatement would not have been detected by the company's internal control over financial reporting; and
 - *Our external auditor has not identified any material misstatements in the current period audit.*
- Ineffective oversight of the company's external financial reporting and internal control over financial reporting by the company's audit committee.
 - *The audit committee has exhibited effective oversight of ICFR*

Based on our assessment of the ineffective ITGCs related to the cyber incident as discussed in Step 1, we assess that these control deficiencies rise to the level of significant deficiency.

Step 6 – Aggregate similar deficiencies and evaluate the aggregated deficiencies for severity

We note the nature of this deficiency at the ITGC level was exposed by and is unique to the cybersecurity event and is likely the result of a control failure that is not typically within the scope of an audit of ICFR. With regard to the FY20 assessment of internal controls, internal audit identified 8 deficiencies related to ITGC operating effectiveness and 3 deficiencies related to design effectiveness. While these deficiencies are not related to the root cause of the cybersecurity event, management considered the potential risk associated with aggregating these deficiencies (See *Appendix C*). For purposes of this evaluation, we noted that the following design deficiency should be aggregated with the deficiencies described in this memo:

- Lack of adequate preventative and/or detective controls over generic accounts to restrict access to financial reporting systems to only approved and authorized users; and,

Attorney Client Privileged / Attorney Work Product

Overall Conclusion

Management concluded that an internal control *significant deficiency* exists in aggregate for 1) authentication and 2) management of generic accounts, and therefore merits attention by those charged with oversight of the company's financial reporting.

Other Considerations

Timing

We note the cybersecurity event was discovered late in the Company's fiscal year and the investigation into the event is on-going. As of the date of this memo, management believes it has sufficient information in order to assess the impact on ICFR and its financial statements, including disclosures.

Remediation

Since the cybersecurity event, we have enhanced authentication requirements and extended our detection and monitoring capabilities through new technology deployments. Because the investigation is ongoing, we anticipate potential additional activities which may further impact remediation planning and control implementation efforts associated with the ICFR control deficiencies noted herein.

Attorney Client Privileged / Attorney Work Product**Appendix C – 2020 ITGC Deficiencies**

Subsidiary	Process	Control Number	Issue Short Name	Rem in 2020?	Effectiveness Level	Impact Consideration
Backup	Change Management	1.2, 1.5	Lack of evidence to show appropriate level of review/approval (Change Mgmt)	Y	Operating Effectiveness	Identified issue was not related to system access
RMM Infrastructure	Change Management	1.2, 1.4, 1.5	Lack of evidence to show appropriate level of review/approval (Change Mgmt)	N	Operating Effectiveness	Identified issue was not related to system access
RMM Infrastructure	Change Management	1.7	Insufficient evidence of control performance, i.e. completeness, timeliness (Change Mgmt)	N	Operating Effectiveness	Identified issue was not related to system access
RMM	Access Provisioning	2.2	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	Y	Operating Effectiveness	Documentation issue only – access was confirmed to be appropriate
NetSuite	Access Provisioning	2.2	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	Y	Operating Effectiveness	Documentation issue only – access was confirmed to be appropriate
Billing Platform	Access Review	2.5	Lack of independent reviewer (Access)	N	Operating Effectiveness	Single individual reviewed themselves
Visual Lease	Access Review	2.5	Lack of independent reviewer (Access)	N	Operating Effectiveness	Single individual reviewed themselves
N-Activate	User Access Management	2.2, 2.5	Incomplete access listing / ineffective review	N	Operating Effectiveness	Single individual inadvertently left out of review
Core IT	Authentication	2.1	Missing attributes relevant to address potential impact of cybersecurity event	N	Design Effectiveness	Primary subject of this memo
Core IT	Generic Account Management	2.5	Lack of specific review performed on underlying access to generic / non-individual accounts	N	Design Effectiveness	Incremental consideration of access to system generic id's is warranted
Netsuite	Privileged Access	A2.5	Users had inappropriate privileged access	N	Operating Effectiveness	There are compensating controls in place to address the risk
Zuora	Access Provisioning	2.2	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	N	Operating Effectiveness	Documentation issue only – access was confirmed to be appropriate
License Orchestration / GL Updater / Zuora Connector	Access Review	2.5	Lack of independent reviewer (Access)	N	Operating Effectiveness	Single individual reviewed themselves
Zuora MSP CA	Privileged Access	A2.5	Users had inappropriate privileged access	Y	Operating Effectiveness	Confirmed no inappropriate activity performed
Backup	Access Review	2.5	Users had inappropriate access	N	Operating Effectiveness	Read-only users had write access